Authenticity of documents in the electronic era

Hoel, Ivar A. L.

Published in:
The 10th Nordic Conference on Information and Documentation Turku, Finland, September 2nd - 4th 1998

Publication date:
1998

Document version
Peer reviewed version

Paper accepted for NordIoD 98, "Facing Information World 2000"
Turku, 2-4. Sept. 1998

Authenticity of documents in the electronic era

by Ivar A. L. Hoel
Royal School of Library and Information Science, Denmark

Abstract:
Taking the story of what happened in the Danish Farum local archives as a starting point, the concept of document authenticity is explained and discussed. In the age of digital documents the original of a document and the copy of it are physically identical and not to be distinguished. Which is the copy, and which is the original? Further, and even more important, altering a few bits in the digital document, making it a new document as it were, does not imply any traceable physical change in the document as such. This opens up to new possibilities fraudulent behaviour as well as to unintended tampering with research results, pieces of historical evidence etc. It makes it necessary to pose the question of how libraries and archives will cope with the new situation. Will they able to guarantee the pristine state of the electronic documents that they keep? It is argued that the role of libraries and archives as institutions in society that can be relied on, to the extent of their guaranteeing the authenticity of documents, must not be underestimated. It is going to be one of their important functions in the future. If the problems which that gives rise to are not taken up and solved, the societal interest in paying for the upkeep of libraries and archives will diminish. The solutions have to take care of organizational, financial and technical problems. Five of the technical possibilites that up to now have been developed are discussed. They are: keeping a log-file, reformatting to secure document media, digital watermarking, digital time-stamping, and asymmetrical encryption.

It is not more than fifteen years ago that copyright was a non-issue for most libraries and other similar information providers. Today it recognized to be of vital importance to our future. The intention of my paper today is to introduce another issue that in my view is going to achieve the same vital importance in the electronic era that we now see the beginnings of. It is the question of *document authenticity*[1].

In other words, I am going to tell you why librarians will have to take an interest in techniques using cryptography or steganography. Perhaps you belong to the happy majority of people that never have heard the last word before. After having heard my paper you will be just a little better informed when you have to decide whether to use it or not. And such decisions will have to be made.

When the concept of authenticity has been discussed in the context of information technology, it has almost exclusively been as the authenticity of a person: who is it that is logging on this server, is he the one he claims to be? etc. What I introduce is a parallel concept of document authenticity. We are going to need it just as much. But before going lexicographical and start defining my words, I will tell you a story.

The Farum story, or: what can happen in an archives
The story is a real life story, and a story that introduces most of the problems related to document authenticity[2]. On January 2nd, 1995 , the telephone in the local history archives of the municipality of Farum, (18.000 inhabitants, situated 20 km north of Copenhagen) rang. That was not unusual. What was unusual was that it was a Copenhagen company, on behalf of a French company, calling. The French company was seeking a patent on something called "enzymatic washing". As the lady in the phone explained, you cannot be granted a patent on something that already has been made known by being published in the press, and during the patenting process it had been claimed that in the local, free weekly newspaper "Farum Folkeblad" there had been an article on just this topic seven years earlier. This was what the Copenhagen company was hired to check, and the question therefore was whether the archives did have a copy of "Folkebladet" dated 1988-01-19. They did. And there it was - a paid-for advertisment on enzymatic washing. Did they want a copy? They certainly did want a certificated copy, and they would then have it translated and sent to Toulouse. The copy having been dispatched, the archives thought that that was the end of the story. But there was more to come.

10 days later a fax from Toulouse arrived. The French company wanted a genuine copy of the newspaper, not just a photocopy. The archives had to fax back and tell that it would be impossible, as they did only have a single copy. Would a copy of the whole newspaper, duly certified, be of interest? It would. The copy having been dispatched, the archives thought that that was the end of the story. But there was more to come. The story has just started.

On May 11th 1995 a chartered accountant from Copenhagen called on the phone. He asked: What kind of newspaper is this, and does it still exist? It did. Wasn't it strange that such an advertisment had appeared in that newspaper? Well, the archives people were not patent experts, so they admitted that they had been more than a trifle curious over the fact that somebody found it worthwhile to pay for the printing of a technical account of L-alpha-amylase. An advertisement for the wonderful suds of some wonderful new household detergent would have been more in style with what their readers expected. How had the archives acquired this newspaper? This was also accounted for. At last came the main question: *Was it possible that somebody could have had a fake copy of the newspaper for that particular day printed, and then smuggled it into the archives, and stolen the original away?* Well, who can downright deny such a possibility? After all, a good patent is worth something, and such a forgery would be much easier than to produce counterfeit money, so…

The very unusual result of such a crucial question was that the local archives made an appeal to the inhabitants of Farum, asking them to look into cellars and attics and report back whether anybody had kept a copy of a seven-and-a-half year old paper - without the infamous advertisement. If that were the case, the forgery would be demonstrated. This appeal to the public gave a result, and showed that the paper in fact was genuine. One of the local readers was employed by a patent office, and she had cut the advertisement out and used it for several years in her teaching as a good example of what is known as "patent prophylaxis". The motives for, and the consequences of this habit that big industrial companies have of laying out minefields for each other is, however, not my concern here. I want to draw attention to the stress that all the way through was put on the question of authenticity, and raise the questions that will be important in the electronic era: *What would have been the outcome of the Farum story if the only copy that had been kept of the newspaper had been stored electronically? How can we in the electronic environment guarantee the document authenticity?*

Document authenticity: a new concept

Since I am introducing the new concept *document authenticity*, I had better explain what I am meaning by it. As for the word document, the old meaning is not fully applicable to what is normally called electronic documents. The issue of whether we by document denote data files, i.e. objects that are locatable and referable to a document carrier, a medium, or whether we by a document also mean screen images of a transitory nature, is an important discussion in its own right.[3] I will not pursue it here, however, as it will not make any great difference for the purposes of this paper[4].

The word authenticity denotes of course the quality of being authentic. That word is derived from greek *authentikós,* which again comes from *authéntes*, meaning perpetrator, doer, author. According to the Oxford English Dictionary the word authentic has four meanings that have a direct bearing on our usage. It may mean

1) authoritative or duly authorized, entitled to obedience or respect,
2) being genuine, proceeding from its reputed source or author,
3) being reliable, trustworthy, of established credit, as opposed to counterfeit, forged,
4) being original, first hand, as opposed to copied.

Remembering the story just told, it is quite clear that the French company was seeking an authentic document in all four meanings of the word. Their questions touched upon all four possible deviations from true authenticity. We see that the quality of a document is intimately connected with its authenticity in this full meaning: A document that really has the origin and the content it claims to have or is recorded as having, a document that is genuine, trustworthy, authoritative, unchanged and thus true in its substance. One of the few writers on this subject, and possibly also the first, Mr. Peter S. Graham of Rutgers University Library, has stated the problem this way:

" The problem may be put in the form of several questions that confront the user of any electronic document (whether it is text, hypertext, audio, graphic, numeric or multimedia information):

- How can I be sure that what I am viewing is what I want to see?

- How do I know that the document I have found is the same one you used and made reference to in your footnote?
- How can I be sure that the document I now use has not been changed since the last time I used it?
- To put it most generally: How can a reader be sure that the document used is the one intended?" [5]

The questions posed are important and apt, but I do, however, have some reservations about the inclusion of the concept of personal intention in the last, generalized question. Document authenticity should be able to be guaranteed without reference to the needs of a specific person.[6]

Traditional documents carry their own history

Peter S. Graham was only speaking of electronic documents. The distinction between traditional and electronic documents is an important distinction when it comes to authenticity. The reason for that has to be explained more fully. The question of document authenticity must have existed from the very first beginning. In traditional document production, however, copies and defect or corrected specimens can be detected, if necessary by scientific analytical methods. Hitler's alleged diaries may be used as an example [7]. Traditional documents cannot be altered without visible or microscopic marks being made. It will for instance normally be easy for an expert using physical analytical methods to decide which of two signatures that was written first, if they are superimposed, to give just one example. In this and many other ways, traditional documents carry their own history.

With digital electronic documents it will need new technical knowledge and new conventions for document handling to identify and prove which is the original, how original it is, and what its history of coming into existence has been. The main problem is that electronic copies are completely identical with the electronic original. Amendments, whether they are intended, accidental or fraudulent, can be difficult both to avoid and to detect. How could Hitler's diaries have been exposed if they had been electronic? What will keep a person from reediting his diaries, memoires, scientific papers etc, given the opportunity? Will not vanity triumph over honesty in a number of cases? How much is scientific, technical, commercial, or social information in a given document to be trusted, if nobody is able to guarantee the authenticity of the document? Document quality is undeniably related to document authenticity. Somebody has to certify the authenticity. With traditional documents, the authenticity could be more or less guaranteed if the physical medium that carried the information was preserved. With electronic documents, the task has become a triple task:

- the document carrier still has to be preserved, often by copying and recopying
- technological obsolescence has to be avoided
- the document must not be tampered with (document integrity)

The trustworthiness of libraries and archives is at stake

The Farum story gives a clue to who that guaranteeing entity could be. Two observations that emerge from the story should be made in order to reveal them.

It is no news that if it were possible to remake history by making changes in existing documents, or contesting their validity, many would have a great interest in doing so. But it may be an overlooked fact that this is not a question only about legal documents, like wills. Libraries and archives have in their possession also a number of anonymous and ephemeral documents. Since they are the very stuff that history are made of, questions will be raised about their authenticity just as well as for "important" documents.

Further, it is very obvious that the archives - and this will apply to libraries and museums as well - was looked upon as an institution that was able to (or at least ought to be able to) give a guarantee that the newspaper indeed was genuine and was not tampered with. We that work in such institutions are surrounded by a feeling in society that we are trustworthy, that we are societal institutions that are to be relied upon. We want to be looked upon as trustworthy institutions. And we deserve it. It is a long tradition with centuries of dedicated work, that has earned us that reputation. Such a reputation is not to be treated lightly. Also in the electronic era we ought to be able to be relied upon.

But that makes it necessary for us to take up the task and come up with some useful solutions. We must master technologies that have been unknown to us earlier. Many things have to be re-engineered, to use a cathcphrase which seems to be especially apt here. If we come to think of it, our situation is not much different from the one that obtained when the printing press was invented. The solutions at that time were not

all at hand, but had to be worked out in a long process. The big difference is that in the 15th century, decades could be used to solve problems that we nowadays have only years or months to adapt to.

In the words of Peter S. Graham, to which I fully subscribe:

"The Digital Research Collection, both for digital images as the focus of this symposium and for digital information generally, must guarantee the longevity and authenticity of information held in trust for present and future generations. Establishing a Digital
Research Collection continues the research library mission. To do so should be considered as natural as acquiring the next book or cataloging the next journal. Not to do so would be an abdication of that mission. The task calls not so much on new knowledge nor on new techniques, but upon informed commitment: that is, upon will. For librarians wondering what is to come of their profession in the electronic age, here is their challenge."[8]

It can be safely said that this aspect of the digital age in libraries and archives has not been overemphasized. It has rather been overlooked. But if we fail to solve the problem, our status as institutions that can guarantee the authenticity of documents is at stake[9]. And who will then pay for the upkeep of such institutions?

So how will we cope with the situation? What are our options? I will mention five possible technical solutions that up to now have been explored by different persons or institutions. A technical solution alone is not enough. It has to be backed by organizational procedures and financial support. This, however, is outside the scope of the present paper.

Five possible technical solutions
The following five possibilities do not necessarily scan the whole field. They represent ideas that have to a lesser or greater extent have been explored by persons interested in the questions raised above, and they are the possibilities that one most readily encounter when searches are made. Within the context of this paper, I will not endeavour to give a complete technical introduction, but only give some explanatory comments and some references for further study of the area.

A. Keeping a log-file
There is a great urge these days to introduce more Information Technology in hospitals. Estimates show that billions of kroner will be used to streamline and modernize the information flow. One of the means will be to introduce electronic case records of the patients. In Denmark, only one small hospital has done so as of May 1998 (Rudkøbing). Sweden, together with the Netherlands, is the European country that so far has done the most. In Scania, all ten hospitals have electronic patient case records[10]. It must be considered vital, in the literal sense, that these records are not tampered with. How is that done?

According to the information I have been able to find in Denmark, it is done by keeping a log-file which makes a record of who has had access to the record, and introduced which changes.[11] It is possible that this is viable in a hospital environment, where the number of persons who are to have access is low and under control.[12] But how can the method possibly be used in the open environment of a research community?

B. Reformatting to secure document media
Archives around the world receive an increasing number of electronic documents that shall be kept for an indefinitely long period of time. One of the possibilities they are exploring is the transfer to other digital media. Making a copy on permanent paper would be technically sound, but economically unfeasible for them because of the sheer mass of data. For smaller amounts of data, the paper option is in fact used[13].

Because of the threat from technical obsolescence of reading devices, the archives have to plan for a remake of the data onto new carriers every five to ten years. That makes a digital solution indispensable. The National Archives in Sweden plan to use CD-R (CD-Recordable) and DAT tapes. The National Archives in Denmark plan to use two CD-R kept in different places[14]. CD-R is a write-once medium (not to be confused with a CD Erasable) that should take care of the authenticity problem[15]. But it is not a practical medium for documents that are to be readily accessible. Its main use will be as a back-up medium from which fresh copies for ordinary, everyday use can be drawn. That will make a check of document authenticity by making comparisons with secure original kept on CD-R a very complicated process. One can easily predict that it will

not be performed except in very special cases. Normally, researchers will not bother to check anything, and when such is the case, many strange things can happen.

A variation of this idea has for several years has been used in the US for commercial electronic documents. Independent companies will act as a disinterested third party and for a certain charge keep a copy of the contract or other document, to be used as reference in case of dispute. The authority of such a procedure will of course be totally dependent on the trustworthiness of the company. It is quite likely that such companies will use CD-R (which were not yet invented when these procedures first started) for document medium.

C. Digital watermarking

Steganograhpy is an old word that suddenly has come into fashion again[16]. It is related to, but not the same as cryptography. Where cryptography is the study and application of principles and techniques by which information is rendered unintelligible to all but the intended receiver[17], steganography is information hiding in a publicly known document in such a way that the hidden information is unknown to or unnoticed by all but the intended receiver. The puzzle pictures (fiksérbilleder) from our childhood provide an example of the idea. The word is constructed out of greek *steganós,* meaning covering, shielding, (water)tight, and *gráphein*, writing. A number of steganographic data programs are available[18]. The steganographic principle is what is used in the recent idea of digital watermarking[19].

A digital watermark is composed of a bit pattern distributed throughout the data to be watermark protected. The distribution is based on noise theory. If done well, no visual or aural degradation should be noticable, as it should be stored in an imperceptible region of the data. The watermark should be more or less indestructible, since it is not purely digital, but a digital representation of analog data. Attempts to remove a watermark form an image will result in a noticeable degradation in image quality long before the watermark is lost.

Until now, digital watermarking has been developed and used mostly for pictures. Embedded in a graphic data file, and hidden to the naked eye, it will provide an identification code carrying information about copyright protection and data authentication. A typical watermark will contain a copyright notification, a unique identification number, a creator identifier, a distributor identifier, a transaction identifier and other data attributes. The watermark can be seen with a viewer that normally is freeware. With a special webcrawler program, watermark owners can search the net for data files containing their own watermark and possibly downloaded and made available without copyright having been achieved. Such things are known to happen. So digital watermarking programs are fort the time being well suited to pursue copyright violation on the Internet. In the future, audio and video files will probably be protected in that way as well. But will they help in the issue of document authenticity as described above? Well, that is an interesting question that should be considered carefully, and research into it should be done.

The two last solutions that I will describe, both make use in some way of the idea of a digital signature. Digital signatures work by attaching to the document an encoded section containing such data as the author's name, the time of encryption and a checksum based on the contents of the document, an possibly other factors, such as the time. The result is that if the document is intercepted or hacked, it cannot be validly altered withot invalidating the checksum.

D. Digital time-stamping

A solution that is expressly invented to meet the challenges listed in this paper has been described by Peter S. Graham[20]. He tells about two researchers from Bellcore, Scott Stornetta and Stuart Haber, who, following up on a discussion of a charge of intellectual fraud (against some third person) set out to find a way of demonstrating that there had been no tampering with electronic evidence. They wanted a solution that was not dependent on hardware, which in due time would be obsolete. Therefore, they opted for an algorithmic solution. It has to be easy to use, so that it does not hinder access and use. It must be cheap and long-lived (much longer than the lifespan of individuals). The authenticity must be demonstrable, and not only inferred. I am not sure whether these criteria were evident from the beginning, but the solution as far as I have seen it described (and I know of it only in that second-hand way) they seem to be met. They called their solution Digital Time Stamping (DTS).

Digital Time Stamping makes use of a cryptographic technique called one-way hashing, which the document in question is subjected to (This does not necessarily mean that the document itself is encrypted, only that a

hash, a single number with many digits calculated with the help of a hash function from the bit string of the document has to be established). It also makes use of a “widely witnessed event”, which draws on the fact that what is known to many people outside the circle of interested parties is more difficult to tamper with. DTS incorporates this by openly intertwining the hash of a given document with the hashes of other documents submitted by unknown other parties. The combined hash for a document obtained this way - the document “certificate” - is the result of a visible chain of actions from a number of parties. The purpose of all this is to make sure not only that a document is kept in its original state, but also that it existed in that state at a certain point in time. A DTS document certificate will thus serve as a documentation of intellectual, financial or legal priority.

To use DTS in practice, it is necessary that there somewhere - in a country or a region perhaps - exists a time-stamping server. The clients will use some simple software with the hash algorithm on their own PC, transmit the hash to the time-stamping server, which then combines the hash with previous hashes. The resulting number (the “certificate”) is sent back to the user and may become part of the document authentication process when that is needed. How much this idea is now starting to be used in practice in the US. In April 1997, Research Libraries Group signed a contract with a Bellcore subsidiary named Surety technologies[21], headed by Scott Stornetta, to provide electronical data validationservices for digital collections. I have never heard of any implementation of it in Europe. But the idea seems to be too good for our purposes to be left unexplored.

E. Asymmetrical encryption

An idea which on the other hand has been put to use in practical work in Scandinavia, is that of employing one of the fringe benefits of an encryption program package. The package in question is PGP, short for Pretty Good Privacy, a program developed in the US by Phil Zimmerman. It has more or less become the de facto standard for encryption within the public domain. Phil Zimmermans work started as a protest against US government wanting in principle to have access to electronic communication between individuals. His idea was that private persons should be able to protect the privacy in their e-mail messages and file attachments by encrypting them, so that only those with a proper authority can decipher the information. Also, the messages can be digitally signed, so that it is ensured they have come from the person who allegedly sent them, and further that they have not been tampered with in any way while in transit. For private persons, PGP is a public domain programme, in full keeping with Zimmermanns point of view.

This is not the place for a discussion of encryption policy, which for the last couple of years has been on the agenda in the EU. Nor is it the place for a discussion of the US policy on the possible export of the strong encryption algorithm used in PGP, which has brought about the situation that it is illegal to download the PGP™ program from a US site (but there are others)[22].

At the heart of PGP is the encryption/decryption, carried out with asymmetrical encryption, using the combined set of a public key and a private key[23]. What in the present connection is interesting, is that PGP furthermore makes use of digital signatures to provide message authentication. Out of the message a “message digest” is made with the help of a strong one-way hash function. This digest can then again be encrypted with the sender’s private key, creating a digital signature of the message. PGP is used by Linköping University Electronic Press to provide article integrity in their electronic journals[24]. PGP has been released in several versions. The latest general release of the international release is PGP5.0i, for Window 95 a release 5.5 3i exists. In earlier versions, a well known algorithm called MD5 for message digest creation was used. The trouble with MD5 is that in 1997, a German data specialist busted the algorithm, making it possible to beat the security of the encrypted signature. For that reason, PGP earned a bad reputation amongst those data people for whom security is of the utmost importance. On the other hand, PGP has now, in version 5.0 and later, found another and reportedly even more secure way of creating a message digest. In any case, PGP must be considered the state-of-the-art for normal, everyday message security. But is that enough for libraries and archives that want to guarantee complete security?

If we do not pursue this and the other questions that I have raised, we will never know. We even run the risk of being out of business if we do not take these issues very seriously. Is that what we want?

[1] Some of my ideas on document authenticity have been published earlier in a Norwegian precursor to this paper, see *Strukturert elektronisk bibliotek eller kaotisk viten, Datalib - 95, Trondheim 24.- 26. oktober 1995, p. 77-89.*

[2] The story has been told in Farum Avis 1995-06-20. Extra information is by personal communication from the Farum archivist, Mr. Bjarne Birkbak.

[3] See *Michael K. Buckland: What is a "Document"?, JASIS 48(9): 804-809, 1997*, for a discussion of meanings of the word document.

[4] As to my personal opinion on this issue, I find that the definition in the Danish "Informationsordbogen. Ordbog for informationshåndtering, bog og bibliotek", published by Danish Standards, 1. ed. 1991 and 2. ed. 1996: "En vis afgrænset mængde af informationer registreret på et medium. Det informationsbærende materiale kan være papir, film, magnetbånd, optiske plader m.m. Dokumentet kan håndteres som enhed i en dokumentationsproces" should be adhered to. Information and medium are inseparably united, making up a document. This may be considered a perfect example of the Aristotelian concepts of form (information, intellectual content), and substance (medium, document carrier), making up a thing (document).

[5] *Peter S. Graham: Long-term intellectual preservation*. URL *http://aultnis.rutgers.edu/texts/dps.html*. Dated July 18, 1995.

[6] In the context of electronic business document security, four concepts have been discussed:

- Integrity, i.e. making sure that nothing in the document has been changed without the reader being made aware of it
- Authentication, i.e. giving the person A - and nobody but A - the possibility of proving to person B that he really is A.
- Confidentiality, i.e. making sure that no third party is able to acquire an understandable message that two contracting parties want to be kept secret.
- Indiscutability, i.e. the possibility for a third party in the role of an umpire to decide what the genuine text is, when two contracting parties disagree as to the content of a document.

This usage is somewhat different from the one I have proposed. In the light of the above usage, it has been discussed in Denmark whether it would be advisable to use the concept of "document integrity" instead of what I have called document authenticity. But integrity is a more restricted concept. The word authenticity is at the same time broader and more precise in describing my intentions. It includes data integrity, but also e.g. presupposes correct cataloguing.

[7] In 1983 the alleged diaries from 1934, 1941 and 1943 were analyzed by Bundesanstalt für Material-forschung und Materialprüfung in Berlin. Microscopic samples from a.o. endpaper and sewing thread were taken. Some of the examples from the findings: All papers were fluorescent in ultraviolet light, but whereas optical whiteners were known from 1930, they were not used in paper (or detergents) before around 1945, because of lack of lightfastness. In the thread, perlon fibres were found. The first German patent for perlon was from June 11th 1938, and it could not have been used in a book from 1934. In the spine lining, fibres of polyethylenterephthalate were found. Such fibres were first made in English laboratories in 1941, and were industrially produced for the first time in Yorkshire in 1953. Thus the inevitable conclusion: forgery! The full account is found in *Dipl-Chem. Barbara Werthmann: Alterungsbestimmungen von Papier und der Nachweis von Fälschungen. 6th IADA Congress, Berlin 5.10 - 9.10. 1987*.

[8] Peter S. Graham, op.cit., Conclusion

[9] Just to mention one example: the increasing use of Publishing-on-demand, a.o. for the production of syllabus material presupposes the authenticity of the electronic documents used.

[10] *Ingeniøren, 24(1998) nr. 16, p. 12-14*

[11] Personal communication from MD Hans Sylvest, Kommunedata.

[12] A widely reported recent Danish case of unauthorized access by policemen to police records (making publicly known a thirty year old case of drunken driving by one of the top Danish politicians) show that even in controlled environment such as the police corps, the use of passwords and logfiles does not guarantee top security.

[13] As an extra security to the option described under letter E, Linköping University Electronic Press makes a paper copy and sends it to two Swedish deposit libraries.

[14] Information given by Jan Danielsen, Statens arkiver, in the presentation "Hva gør vi for at sikre bevaringen af det digitaliserede materiale?" in a symposion arranged by Kulturnet Danmark, Copenhagen 1998-04-29.

[15] The question of the lifetime of a CD-ROM and a CD-R is in that context of great importance. Tha fact is that nobody knows whether it is 10 or 100+ years, or, rather, when it is 10 and when it is 100+. An International Standard with the title "*Life expectancy of compact discs (CD-ROM) - Method for estimating, based on effects of temperature and humidity*" is on its way, but it will not cover CD-Recordable.

[16] Out of 13 of the world's great encyclopedias, only the two oldest (The Danish Salmonsen 2.ed from around the First World War and Enciclopedia Italiana from the thirties) recognized the word in the form of a reference to other articles. A search for the word in Alta Vista will give thousands of references.

[17] Encycl. Brit. 15. ed. Vol.3 p. 768

[18] For more information on steganography, try Neil F. Johnsons homepage, URL *http://patriot.net/~johnson/Steganography/*, with many links to articles and other sites. On the URL *http://www.heise.de/ct/pgpCA/stego.shtml* references to twenty steganographic programs may be found, with names like Steganosaurus, Hide and Seek, White Noise Storm and others. Not all of them are truly steganographical, not all of them are good, and only two will work on other than picture files.

[19] Three links to companies selling digital watermarking programs:
The Dice Company: *http://www.digital-watermark.com/*
Digimarc Corporation: *http://www.digimarc.com*
Signum Technologies: *http://www.signumtech.com*

[20] op.cit,and also in his *Intellectual Preservation: Electronic Preservation of the Third Kind* (Washington DC, Commission of Preservation and Access, March 1994)

[21] For more information, see URL *http://www.surety.com*. The company licenses a program called Digital Notary ™ Record Integrity Service.

[22] From the URL *http://www.pgpi.com* you will find all necessary information on the international version of PGP. If you want to follow the US side of it URL http://www.pgp.com, or after the merger of PGP with McAfee and other to make Network Associates, *http://www.nai.com/default_pgp.asp*.

[23] Asymmetrical encryption, with the use of a private key which is kept secret by the owner, and a public key which is made known to all likely recipients of messages sent by the owner of the private key, will not be described here. For one of easiest understandable but still technically sound explanations of what it is, see the chapter Phil Zimmermann has written in the official PGP User's Guide, which may be downloaded from the URL mentioned above, or in one of the books on PGP, *William Stallings: Protect your privacy. A guide for PGP users. Prentice Hall PTR 1995. 302 pp. ISBN 0-13-185596-4*

[24] See URL *http://www.ida.liu.se/ext/cgi-bin/epa/protect.html* for more information.